THE ASSISTANT COMMISSIONER OF PATENTS
Washington, D.C. 20231

DOCKET NUMBER: RPS920000026US1
August 29, 2000

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor: Barry Atkins et al.

For: SYSTEM, METHOD, AND PROGRAM FOR MANAGING A USER KEY USED TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM

Enclosed are:

_X_   Patent Specification and Declaration

_X_   _4_   sheets of drawing(s).

_X_   An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).

_   A certified copy of a Japan application.

__   Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				$690
Total Claims	24 - 20	4	x 18 =	$ 72
Indep. Claims	3 - 3		x 78 =	$
MULTIPLE DEPENDENT CLAIM PRESENTED			x 270 =	$
			TOTAL	$762.00

_X_ Please charge IBM Corporation Deposit Account No. 50-0563 in the amount of $762.00.   A duplicate copy of this sheet is enclosed.

_X_ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 50-0563.   A duplicate copy of this sheet is enclosed.

_X_ Any additional filing fees required under 37 CFR §1.16.

_X_ Any patent application processing fees under 37 CFR §1.17.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" mailing label number EL453463173US

Date of Mailing August 29, 2000

I hereby certify that the documents indicated below are being deposited with the United States Postal Service under 37 CFR 1 10 on the date indicated above and are addressed to Box Patent Applications, Assistant Commissioner of Patents, Washington, D C 20231 and mailed on the above Date of Mailing with the above "Express Mail" mailing label number

Marty Bower

Respectfully submitted,

Brian F. Russell

By
Brian F. Russell, Registration No. 40,796
FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP
Suite 350 Lakewood on the Park
7600B North Capital of Texas Highway
Austin, Texas 78731
Telephone (512) 343-6116

SYSTEM, METHOD, AND PROGRAM FOR MANAGING A USER KEY USED TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM

BACKGROUND OF THE INVENTION

1.   Technical Field:

The present invention relates in general to data processing, and, in particular, to a system, method, and program for providing data security. Still more particularly, the present invention relates to a system, method, and program for managing a user key used to sign a message for a data processing system.

2.   Description of the Related Art:

Cryptography involves encrypting data to provide security for the data. For example, before transmission of a message from one party to another, the message may be encrypted using a mathematical function known as a cryptographic algorithm. The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key" is required to decrypt an encrypted message. Two prevalent types of key-based cryptographic algorithms exist, namely, *symmetric key* (or secret key) algorithms and *public key* (asymmetric key) algorithms. The security provided by these cryptographic algorithms is centered around the keys and not the details of the cryptographic algorithms. In other words, the cryptographic algorithms can typically be known to all, but the keys can only be known by authorized parties. As a result, the cryptographic algorithm may be published for public scrutiny and then mass produced for incorporation

into security products.

In most symmetric key algorithms, the encryption key
and the decryption key are the same secret key. The
sender and recipient of a message must be able to exchange
information regarding the secret key, and each party must
trust the other not to disclose the secret key. The
sender must communicate the key through another relatively
secure communication path. With public key algorithms,
the key used for encryption is different from the key used
for decryption. The decryption key is difficult to
calculate from an encryption key. In a typical operation,
the public key used for encryption is made public via a
readily accessible directory, while the corresponding
private key used for decryption is known only to the
recipient of the encrypted message. In an exemplary
public key transaction, a sender retrieves the recipient's
public key and uses it to sign the message prior to
sending the message. The recipient then receives and
decrypts the encrypted message with the corresponding
private key. Encrypting a message using a private key and
decrypting the encrypted message using a public key, which
is sometimes used in digital signatures to authenticate
the source of a message, are possible.

One of the more popular public key algorithms is RSA
(named after its inventors Rivest, Shamir, and Adleman).
With RSA, when a message is encrypted utilizing a user
public key, the encrypted message may only be decrypted
utilizing a user private key. In one implementation, each
user private key is also associated with a password, and
both are enclosed within an individual secure wrapper.
All user private keys along with their respective

passwords are stored in a protected storage area within an
encryption/decryption device, such as an encryption chip.
In order to allow the encryption chip to perform an
authentication procedure, such as signing signatures, a
user must provide a correct password to the encryption
chip. For security purposes, copies of any user private
key must not exist outside the secure wrapper. Thus, a
user private key and its respective password can only be
unwrapped inside the encryption chip, leaving no
opportunity for the password to be changed.

Public-private key cryptography allows messages to be
digitally signed. A sender may publish his decryption key
as a public key and maintain his encryption key secret as
a private key. If the sender encrypts a message using the
private key, then anyone receiving the message is able to
decrypt the message using the sender's public key. In
doing so, the recipients are able to verify that the
message was encrypted by the sender since he is the sole
possessor of the private key. The sender has, in effect,
digitally signed the message. An alternative way of
digitally signing a message involves the use of a hashing
function, which is also known as a "message digest" or
"fingerprint" algorithm. A message is hashed using a
cryptographic hash function. The cryptographic hash
function maps an arbitrary-length message to a fixed
number of bits. The hashed message or hash is then
encrypted. Digitally signing a message using the hashing
function is generally a two-step process. The first step
involves hashing the message and encrypting the hashed
message using a private key. The message is transmitted
along with the encrypted hash from the sender to the
recipient. The second step involves the verification of

the signature. The recipient hashes the received message, decrypts the received, encrypted hash with the associated public key and compares the pair of hashed values. The signature is valid if the two hashed values match. Otherwise, the message was somehow altered during transmission.

Certification is the process of binding a key, such as a public key or private key, to an individual, organization, entity, or piece of information, such as a permission or credential. A certificate is a collection of information that has been digitally signed by a certificate issuer. The certificate issuer is a party who issues a key to a person, organization, entity, or piece of information and manages the validity of the issued key. If a user is no longer permitted to use a key, the certificate issuer needs to revoke the certificate for the user's key by publishing the certificate for the key on a certificate revocation list ("CRL"). However, a time gap typically exists between when a certificate issuer receives a notification that a certificate for a key should be revoked and when the certificate issuer publishes the certificate of the key on the next CRL. This time gap results in what is known as the CRL time-granularity problem. During this time period, the user may attempt to use the key to engage in unauthorized transactions and communications that should have been invalidated by the revocation of the key and the certificate for the key. The user may then continue to sign messages and communicate without proper authority. The present invention recognizes the need and desire to resolve this problem.

SUMMARY OF THE INVENTION

A system, method, and program for managing a user key
used to sign a message for a data processing system having
an encryption chip are disclosed. A user is assigned a
user key. In order to encrypt and send messages to a
recipient(s), the messages are encrypted with the user
key. The user key, in turn, is encrypted with an
associated key. The associated key is further encrypted
using an encryption chip key stored on the encryption
chip. The encrypted messages are communicated to a
recipient to validate an association of the user with the
encrypted messages. The associated key is decrypted with
the encryption chip key. The user key is decrypted with
the associated key, and the messages are decrypted with
the user key. Thereafter, validation of the association
of messages with the user is removed by revoking the
associated key.

In a preferred embodiment, encryption resources are
centralized in a server system having the encryption chip.
The server system is coupled to and provides encryption
services to a plurality of client systems. Messages to be
encrypted are sent from a user's client system to the
server system, which encrypts the messages using the
encryption chip. The encrypted messages are sent from the
server system to the client system, which then transmits
the encrypted messages to their intended recipient(s).
All data relating to the encrypted messages are erased
from the server system after the encrypted messages are
sent from the server system to the client system.

The above as well as additional objects, features,

and advantages of the present invention will become
apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the
invention are set forth in the appended claims. The
invention itself however, as well as a preferred mode of
use, further objects and advantages thereof, will best be
understood by reference to the following detailed
description of an illustrative embodiment when read in
conjunction with the accompanying drawings, wherein:

Figure 1 is an exemplary block diagram of a data
processing system that implements the present invention;

Figure 2 is an exemplary block diagram of a data
processing sub-system, which may be the client system or
server system of **Figure 1,** that implements the present
invention;

Figure 3 is a flow chart of an exemplary method and
program executed by the data processing system of **Figure 1**
for encrypting messages in accordance with the present
invention; and

Figure 4 is a flow chart of an exemplary method and
program executed by the data processing system of **Figure 1**
for decrypting messages in accordance with the present
invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENT

In conventional computer systems,
encryption/decryption of messages are preformed utilizing
an internal encryption chip that stores both the
encryption/decryption algorithms and a key or key pair
used by the encryption chip to encrypt and decrypt data.
In a network environment each computer's encryption chip
performs the same basic encryption/decryption functions,
which invites the consolidation of the
encryption/decryption function at a centralized location
in order to reduce expense and management and enhance
physical security.

However, centralization of encryption and decryption
services at an encryption server can lead to various
problems. One problem is that very secure communication
must be established between each client system and
encryption the server. Otherwise, unauthorized persons
may gain illicit entry to and illegally decrypt encrypted
data communicated between the client systems and the
encryption server. Another problem that arises is
difficulty in key management. A client system is assigned
a key that is provided to the user of that client system.
Various keys for various client systems are used and
managed by the single encryption server. However, if the
issued key for a particular client system needs to be
revoked, the user may maintain a copy of the revoked key
and thereby gain unlawful access to encrypted data by
simply logging into the encryption server from a remote
client system. The present invention consolidates the
encryption/decryption operations of data to a centralized
location while avoiding the problems associated with
centralizing the encryption/decryption operations.

With reference now to **Figure 1,** an exemplary block
diagram of a data processing system **100** that implements
the present invention is shown. Data processing system
100 includes client systems **102A, 102B,** and **102C** coupled

5   in communication with a server system **104.** Communication
between client systems **102A, 102B,** and **102C** and server
system **104** is conducted via a secure communication link,
such as a Secure Sockets Layer ("SSL") connection. SSL is
a standard developed by Netscape Communications for

10   establishing secure communication channels between devices
to avoid interception and unauthorized access of critical
or sensitive data. Client system **102A** has a memory system
103A and a central processing unit (CPU) **114A,** which are
coupled to each other. Similarly, client system **102B**

15   includes a memory system **103B** and a CPU **114B,** and client
system **102C** contains a memory system **103C** and a CPU **114C.**
User 1 uses client system **102A,** and user 2 utilizes client
system **102B.** Furthermore, user 3 uses client system **102C.**
The term "user" is understood to mean a person, a service,

20   an application, a device, or any other entity that may
access an application. The term "user" is not limited to
a human user.

Server system **104** has a memory device **105** and a CPU

25   **116,** which are coupled to each other as well. Server
system **104** further includes an encryption chip **106.**
Encryption chip **106,** which is coupled in communication
with CPU **116** and memory device **105,** contains an
encryption/decryption engine ("ENG") **118** and a protected

30   storage ("PS") area **120.** Encryption/decryption engine **118**
implements an encryption/decryption algorithm that encodes
and decodes messages transmitted and received by client
systems **102A, 102B,** and **102C,** in accordance with the

present invention.

In **Figure 1**, users 1, 2, and 3 utilize data
processing system **100** to encrypt messages, such as to sign
messages, that are then electronically transmitted to a
recipient **112** through a recipient system **110**. The present
invention preferably implements a public/private key
encryption and decryption scheme. Key 1, which includes a
public key 1 ("PUK1") and a private key 1 ("PRK1"), is a
user key assigned to user 1. Key 1 is stored in memory
system **103A**. Also, key 2, which includes a public key 2
("PUK2") and a private key 2 ("PRK2"), is issued as the
user key for user 2, and key 2 is stored in memory system
103B. Additionally, key 3, which includes a public key 3
("PUK3") and a private key 3 ("PRK3"), is assigned as the
user key for user 3. Key 3 is stored in memory system
103C. When data processing system **100** performs
encryption/decryption operations, keys 1, 2, and/or 3 are
sent to protected storage area **120** of server system **104**.

Protected storage area **120** may be implemented with an
electronically erasable storage device. Protected storage
area **120** encompasses memory device **105** and an encryption
chip key **107** ("ECK"). Protected storage area **120** stores
the user public/private key pairs. User public/private
key pairs sent to and/or stored within protected storage
area **120** are protected by encryption/decryption engine **118**
and are not directly accessible to server system **104** or
its other components.

In server system **104**, keys A, B, and C (also referred
to as "associated keys") are stored in memory device **105**.
Key A contains a public key A ("PUKA") and a private key A

("PRKA"), and key A is an associated key that is
specifically associated with key 1. Key B includes a
public key B ("PUKB") and a private key B ("PRKB"), and
key B is an associated key that is particularly associated
with key 2. Also, key C contains a public key C ("PUKC")
and a private key C ("PRKC"), and key C is an associated
key that is associated with key 3. ECK **107** has a public
ECK ("PUECK") and a private ECK ("PRECK") and is utilized
to encrypt associated key A, B, or C, and associated keys
A, B, and C in turn are respectively utilized to encrypt
user keys 1, 2, and 3. User keys 1, 2, and 3 encrypt or
sign messages sent by users 1, 2, and 3, respectively.

As stated earlier, certification is the process of
binding a key, such as a public key or private key, to an
individual, organization, entity, or piece of information,
such as a permission or credential. A certificate is a
collection of information that has been digitally signed
by a certificate issuer. A certificate may be established
within a client system, such as client system **102A, 102B,**
or **102C,** for a user, such as user 1, 2, or 3, to access a
particular application. The certificate may be
specifically established for and associated with a
particular user and a particular application. The
certificate preferably includes a pointer to its
associated application, an identity of the user associated
with this certificate, and a pointer to the user private
key associated with the user of this certificate and
application. When an application needs to transmit an
encrypted message or to perform an authentication
procedure, encryption/decryption engine **118** accesses the
user private key pointed to by the application's
associated certificate, and then encrypts the message or
generates a digital signature utilizing the user private

key.

The certificate issuer is a person who issues a key and manages the validity of the key issued to a person, organization, entity, or piece of information. The keys for data processing system **100** are issued by a certificate issuer(s). The certificate issuer manages the validity of the keys by issuing certificates that validate the use of the keys. If a key is to be revoked, then the certificate issuer revokes the key by publishing the certificate for the key on a certificate revocation list. Users 1, 2, and 3 are the certificate users who use the certificates.

Referring now to **Figure 2,** a block diagram of a computer system **10,** which may be client system **102A, 102B,** or **102C** or server system **104,** in which a preferred embodiment of the present invention is implemented is shown. As shown, a processor (CPU) **12,** a read-only memory (ROM) **13,** and a random access memory (RAM) **14** are connected to a system bus **11** of a computer system **10.** CPU **12** may be CPU **114A, 114B,** or **114C** for respective client system **102A, 102B,** or **102C** or may be CPU **116** for server system **104.** CPU **12,** ROM **13,** and RAM **14** are also coupled to a PCI bus **20** of computer system **10** through a PCI host bridge **15.** PCI host bridge **15** provides a low latency path through which CPU **12** may directly access PCI devices mapped anywhere within bus memory and/or I/O address spaces. PCI host bridge **15** also provides a high bandwidth path allowing PCI devices to directly access RAM **14.**

Also attached to PCI bus **20** is a local-area network (LAN) interface **16** and a small computer system interface (SCSI) **18.** LAN interface **16** connects computer system **10**

to LAN **17**.   SCSI **18** is utilized to control a high-speed
SCSI disk drive **19**.   Expansion bus bridge **45**, such as a
PCI-to-ISA bus bridge, may be utilized to couple an ISA
bus **25** to PCI bus **20**.   As shown, a keyboard **26**, a
microphone **27**, a mouse **28**, and a storage device **29** may be
attached to ISA bus **25** to perform basic I/O functions.
Storage device **29** may be memory system **103A**, **103B**, or **103C**
for respective client system **102A**, **102B**, or **102C** or may be
memory device **105** for server system **104**.   In addition, an
audio adapter **23** and a graphics adapter **21** may be attached
to PCI bus **20**.   Graphics adapter **21** controls visual output
through a display monitor **22** and audio adapter **23** controls
audio output through a speaker **24**.

With reference now to **Figures 3** and **4**, flow charts of
exemplary methods **300** and **400** and programs executed by
data processing system **100** for encrypting and decrypting
messages in accordance with the present invention are
shown.   Methods **300** and **400** will be discussed in
conjunction with an example for digitally signing a
message hashed by a cryptographic function.   The hashed
message is sent by user 1 and encrypted and decrypted by
methods **300** and **400** utilizing user key 1, associated key
A, and ECK **107**.   Methods **300** and **400** are not in any way
limited to this exemplary application.   Methods **300** and
400 encrypt and decrypt messages in the same manner for
users 2 and 3 using user keys 2 and 3, associated keys B
and C, and ECK 107.   Methods **300** and **400** may be used to
encrypt/decrypt any suitable messages.

As shown in **Figure 3**, method **300** for encrypting
messages in accordance with the present invention starts

at block **302**. Method **300** next moves to block **304**, which
illustrates user 1 being assigned user key 1. User 1 uses
user key 1 to encrypt or sign messages that are processed
by data processing system **100**. Following block **304**, block
305 shows a message sent by user 1 being hashed by a
cryptographic hash function in client system **102A**.
Method **300** next moves to block **306**, which shows that the
hashed message is encrypted with user key 1 in client
system **102A**.

Following block **306**, block **308** depicts the hashed
message encrypted by PRK1 of user key 1 being sent from
client system **102A** to server system **104**. The encrypted,
hashed message includes the identity of user key 1, which
is, in effect, transmitted from client system **102A** to
server system **104** when the encrypted, hashed message is
sent. Any personal identification numbers (PINs) or
passwords associated with using user key 1 are also sent
from client system **102A** to server system **104**. User key 1
and all associated PINs or passwords, if any, are received
and securely maintained within protected storage area **120**
of server system **104**.

Method **300** then moves to blocks **310**, **312**, and **314**.
Block **310** illustrates server system **104** encrypting user
key 1 with PRKA of associated key A stored in server
system **104**. Following block **310**, block **312** shows server
system **104** encrypting associated key A with PRECK of ECK
107. Method **300** next proceeds to block **314**, which depicts
server system **104** sending the encrypted, hashed message,
encrypted user key 1, and encrypted associated key A to
client system **102A**.

Method **300** moves from block **314** to block **316**, which shows that any trace of the encrypted, hashed message, user key 1, and the associated PINs/passwords are erased from server system **104**. Following block **316**, block **318** shows client system **102A** electronically transmitting the encrypted, hashed message in conjunction with encrypted user key 1 and encrypted associated key A to a recipient system **110**. The encrypted message includes the original message. Recipient system **110** receives the encrypted, hashed message (which includes the message of user 1 whether tampered with or not), encrypted user key 1, and encrypted associated key A. Recipient **112** uses recipient system **110** to decrypt the encrypted, hashed message in order to validate an association of user 1 with the encrypted, hashed message.

Method **300** then proceeds to block **320**. Block **320** illustrates that if revocation of user key 1 for user 1 is desired (e.g., user 1 is no longer employed at the company maintaining data processing system **100** and validation of user key 1 needs to be revoked), then validation of encrypted, hashed messages associated with user 1 can be prevented by revoking associated key A on server system **104**. Associated keys, such as associated keys A, B, and C, are never used outside of server system **104** and are generally only accessed and managed by an authorized system administrator. Associated key A may be revoked by simply erasing it from server system **104**. Since associated key A is revoked and no longer exists in server system **104**, then ECK **107** does not have an associated key to decrypt, and encrypted user key 1, in turn, cannot be decrypted since associated key A does not exist to decrypt user key 1. Method **300** finally ends at block **322**.

In **Figure 4**, method **400** for decrypting messages in accordance with the present invention starts at block **402**. Method **400** proceeds from block **402** to block **403**, which depicts communication being established and maintained between data processing system **100** and recipient system **110**. Following block **403**, block **404** illustrates recipient system **110** receiving from client system **102A** the encrypted, hashed message, encrypted user key 1, and encrypted associated key A. Recipient **112** uses recipient system **110** to validate an association of user 1 with the encrypted, hashed message.

Method **400** then proceeds to blocks **408**, **410**, and **412**. Block **408** represents recipient system **110** decrypting encrypted associated key A by accessing and using PUECK of ECK **107**. Block **410** illustrates recipient system **110** decrypting encrypted user key 1 by accessing and using PUKA of associated key A. Block **412** shows recipient system **110** decrypting the encrypted, hashed message by accessing and using PUK1 of user key 1. Method **400** next proceeds to block **414**, which depicts recipient system **110** accessing and using the same cryptographic hash function used by client system **102A** to hash the message attached to the encrypted, hashed message received from user 1 through client system **102A**.

Method **400** then moves to decision block **416**, which shows a determination of whether the hashed message generated by recipient system **110** is the same as the decrypted hashed message. If a determination is made at decision block **416** that the hashed messages are the same, then method **400** proceeds from decision block **416** to block **418**, which depicts recipient system **110** notifying

recipient **112** that the received message is valid and is
verified as being sent from user 1. On the other hand, if
at decision block **416** the hashed messages are not the
same, then method **400** instead proceeds from decision block
416 to block **420**, which illustrates recipient system **110**
notifying recipient **112** that the received message is not
valid and is not verified as being sent from user 1.
Method **400** finally ends at block **422**.

As has been described, the present invention
discloses a system, method, and program for managing a
user key used to sign a message for a data processing
system having an encryption chip. The present invention
helps prevent unauthorized transactions and communications
from occurring due to the CRL time-granularity problem.
The present invention consolidates the
encryption/decryption function at a centralized location.
The present invention further discloses use of secure
communication and a key revocation scheme to resolve the
problems associated with centralizing the
encryption/decryption function.

While the invention has been particularly shown and
described with reference to a preferred embodiment, it
will be understood by those skilled in the art that
various changes in form and detail may be made therein
without departing from the spirit and scope of the
invention. For example, although aspects of the present
invention have been described with respect to a computer
system executing software that directs the functions of
the present invention, it should be understood that
present invention may alternatively be implemented as a
program product for use with a data processing system.
Programs defining the functions of the present invention

can be delivered to a data processing system via a variety

of signal-bearing media, which include, without

limitation, non-rewritable storage media (e.g., CD-ROM),

rewritable storage media (e.g., a floppy diskette or hard

5   disk drive), and communication media, such as digital and

analog networks. It should be understood, therefore, that

such signal-bearing media, when carrying or encoding

computer readable instructions that direct the functions

of the present invention, represent alternative

10   embodiments of the present invention.

CLAIMS:

What is claimed is:

1   1.   A method for managing a user key used to sign a
2   message for a data processing system, said method
3   comprising:

4   assigning a user key to a user and storing the user
5   key in a data processing system for encrypting messages;

6   encrypting the messages with the user key;

7   storing an associated key in the data processing
8   system and encrypting the user key with the associated key
9   to obtain an encrypted user key;

10   communicating encrypted messages in conjunction with
11   the encrypted user key to validate an association of the
12   user with the encrypted messages; and

13   thereafter, preventing validation of the association
14   of the user with messages by revoking the associated key.

1   2.   The method according to Claim 1, further comprising:

2   decrypting the user key with the associated key; and

3   decrypting the messages with the user key.

1   3.   The method according to Claim 1, wherein the data
2   processing system further comprises a client system having
3   a client memory device coupled to a server system having
4   an encryption chip and a server memory device and wherein:

5   storing the user key in a data processing system for
6   encrypting messages further comprises storing the user key
7   in the client memory device;

8   storing the associated key in the data processing
9   system further comprises storing the associated key in the
10   server memory device; and

11   preventing validation further comprises preventing
12   the validation of the messages associated with the user by
13   eliminating the associated key from the server memory
14   device.

1   4.   The method according to Claim 3, wherein encrypting
2   the messages further comprises:

3   sending the messages to be encrypted from the client
4   system to the server system;

5   encrypting the messages using the encryption chip of
6   the server system; and

7   sending the encrypted messages from the server system

8   to the client system.

1   5.   The method according to Claim 4, further comprising:

2   erasing from the server system all data relating to
3   the encrypted messages after the encrypted messages are
4   sent from the server system to the client system.

1   6.   The method according to Claim 1, further comprising:

2   encrypting the associated key by using an encryption
3   chip key which is stored on an encryption chip of the data
4   processing system.

1   7.   The method according to Claim 6, further comprising:

2   encrypting the associated key with the encryption
3   chip key; and

4   communicating an encrypted associated key to validate
5   the association of the user with the encrypted messages.

1   8.   The method according to Claim 7, further comprising:

2   decrypting the associated key with the encryption
3   chip key.

1   9.   A system for managing a user key used to sign a

2   message for a data processing system, said system

3   comprising:

4   means for assigning a user key to a user and storing

5   the user key in a data processing system for encrypting

6   messages;

7   means for encrypting the messages with the user key;

8   means for storing an associated key in the data

9   processing system and encrypting the user key with the

10   associated key to obtain an encrypted user key;

11   means for communicating encrypted messages in

12   conjunction with the encrypted user key to validate an

13   association of the user with the encrypted messages; and

14   means for thereafter preventing validation of the

15   association of the user with messages by revoking the

16   associated key.

1   10.   The system according to Claim 9, further comprising:

2   means for decrypting the user key with the associated
3   key; and

4   means for decrypting the messages with the user key.

1   11.   The system according to Claim 9, wherein the data
2   processing system further comprises a client system having
3   a client memory device coupled to a server system having
4   an encryption chip and a server memory device and wherein:

5   said means for storing the user key in a data
6   processing system for encrypting messages further
7   comprises means for storing the user key in the client
8   memory device;

9   said means for storing the associated key in the data
10   processing system further comprises means for storing the
11   associated key in the server memory device; and

12   said means for preventing validation further
13   comprises means for preventing the validation of the
14   messages associated with the user by eliminating the
15   associated key from the server memory device.

1   12.   The system according to Claim 11, wherein said means
2   for encrypting the messages further comprises:

3   means for sending the messages to be encrypted from
4   the client system to the server system;

5   means for encrypting the messages using the
6   encryption chip of the server system; and

7   means for sending the encrypted messages from the

8   server system to the client system.

1   13. The system according to Claim 12, further comprising:

2   means for erasing from the server system all data

3   relating to the encrypted messages after the encrypted

4   messages are sent from the server system to the client

5   system.

1   14. The system according to Claim 9, further comprising:

2   means for encrypting the associated key by using an

3   encryption chip key which is stored on an encryption chip

4   of the data processing system.

1   15. The system according to Claim 14, further comprising:

2   means for encrypting the associated key with the

3   encryption chip key; and

4   means for communicating an encrypted associated key

5   to validate the association of the user with the encrypted

6   messages.

1   16. The system according to Claim 15, further comprising:

2   means for decrypting the associated key with the

3   encryption chip key.

1   17. A program product for managing a user key used to

2   sign a message for a data processing system, said program

3   product comprising:

4   a control program including:

5   instruction means for assigning a user key to a user
6   and storing the user key in a data processing system for
7   encrypting messages;

8   instruction means for encrypting the messages with
9   the user key;

10   instruction means for storing an associated key in
11   the data processing system and encrypting the user key
12   with the associated key to obtain an encrypted user key;

13   instruction means for communicating encrypted
14   messages in conjunction with the encrypted user key to
15   validate an association of the user with the encrypted
16   messages;

17   instruction means for thereafter preventing
18   validation of the association of the user with messages by
19   revoking the associated key; and

20   computer usable media bearing said control program.

1   18. The program product according to Claim 17, further

2   comprising:

3   instruction means for decrypting the user key with

4   the associated key; and

5   instruction means for decrypting the messages with

6   the user key.

1   19. The program product according to Claim 17, wherein

2   the data processing system further comprises a client

3   system having a client memory device coupled to a server

4   system having an encryption chip and a server memory

5   device and wherein:

6   said instruction means for storing the user key in a

7   data processing system for encrypting messages further

8   comprises instruction means for storing the user key in

9   the client memory device;

10   said instruction means for storing the associated key

11   in the data processing system further comprises

12   instruction means for storing the associated key in the

13   server memory device; and

14   said instruction means for preventing validation

15   further comprises instruction means for preventing the

16   validation of the messages associated with the user by

17   eliminating the associated key from the server memory

18   device.

1   20. The program product according to Claim 19, wherein

2   said instruction means for encrypting the messages further

3   comprises:

4   instruction means for sending the messages to be

5   encrypted from the client system to the server system;

6   instruction means for encrypting the messages using

7   the encryption chip of the server system; and

8   instruction means for sending the encrypted messages

9   from the server system to the client system.

1   21. The program product according to Claim 20, further

2   comprising:

3   instruction means for erasing from the server system

4   all data relating to the encrypted messages after the

5   encrypted messages are sent from the server system to the

6   client system.

1   22. The program product according to Claim 17, further

2   comprising:

3   instruction means for encrypting the associated key

4   by using an encryption chip key which is stored on an

5   encryption chip of the data processing system.

1   23. The program product according to Claim 22, further

2   comprising:

3   instruction means for encrypting the associated key

4   with the encryption chip key; and

5   instruction means for communicating an encrypted

6   associated key to validate the association of the user

7   with the encrypted messages.

1   24.   The program product according to Claim 23, further
2   comprising:

3   instruction means for decrypting the associated key
4   with the encryption chip key.

ABSTRACT OF THE DISCLOSURE
SYSTEM, METHOD, AND PROGRAM FOR MANAGING A USER KEY USED
TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM

5   A system, method, and program for managing a user key
used to sign a message for a data processing system having
an encryption chip are disclosed. A user is assigned a
user key. In order to encrypt and send messages to a
recipient(s), the messages are encrypted with the user
10   key. The user key, in turn, is encrypted with an
associated key. The associated key is further encrypted
using an encryption chip key stored on the encryption
chip. The encrypted messages are communicated to a
recipient to validate an association of the user with the
15   encrypted messages. The associated key is decrypted with
the encryption chip key. The user key is decrypted with
the associated key, and the messages are decrypted with
the user key. Thereafter, validation of the association
of messages with the user is removed by revoking the
20   associated key. In a preferred embodiment, encryption
resources are centralized in a server system having the
encryption chip. The server system is coupled to and
provides encryption services to a plurality of client
systems. Messages to be encrypted are sent from a user's
25   client system to the server system, which encrypts the
messages using the encryption chip. The encrypted
messages are sent from the server system to the client
system, which then transmits the encrypted messages to
their intended recipient(s). All data relating to the
30   encrypted messages are erased from the server system after
the encrypted messages are sent from the server system to
the client system.

FIGURE 1

FIGURE 2

SCSI ~18
~19

LAN INTERFACE ~16
~17

PCI BUS ~20

PCI HOST BRIDGE ~15

CPU ~12

ROM ~13

DRAM ~14

SYSTEM BUS ~11

~10

EXPANSION BUS BRIDGE ~45

ISA BUS ~25

GRAPHICS ~21

~22

AUDIO ~23

~24

~26

~27

~28

~29

300

302 → (START)

304 → USER 1 IS ASSIGNED USER KEY 1 THAT IS USED TO ENCRYPT OR SIGN MESSAGES PROCESSED BY A DATA PROCESSING SYSTEM 100.

305 → A MESSAGE SENT BY USER 1 IS HASHED BY CRYPTOGRAPHIC HASH FUNCTION IN CLIENT SYSTEM 102A.

306 → HASHED, MESSAGE IS ENCRYPTED WITH PRK1 OF USER KEY 1 IN CLIENT SYSTEM 102A.

308 → ENCRYPTED, HASHED MESSAGE, THAT HAS THE IDENTITY OF USER KEY 1, AND PINs ARE SENT BY USER 1 FROM CLIENT SYSTEM 102A TO SERVER SYSTEM 104.

310 → SERVER SYSTEM 104 ENCRYPTS USER KEY 1 WITH PRKA OF ASSOCIATED KEY A STORED IN SERVER SYSTEM 104.

312 → SERVER SYSTEM 104 ENCRYPTS ASSOCIATED KEY WITH PRECK OF ECK 107.

314 → SERVER SYSTEM 104 SENDS ENCRYPTED, HASHED MESSAGE, ENCRYPTED USER KEY 1, AND ENCRYPTED ASSOCIATED KEY A TO CLIENT SYSTEM 102A.

316 → ANY TRACE OF ENCRYPTED, HASHED MESSAGE, USER KEY 1, AND PINs ARE EREASED FROM SERVER SYSTEM 104.

318 → CLIENT SYSTEM 102A ELECTRONICALLY TRANSMITS THE ENCRYPTED, HASHED MESSAGE, ENCRYPTED USER KEY 1, AND ENCRYPTED ASSOCIATED KEY A TO RECIPIENT SYSTEM 110 TO VALIDATE BY RECIPIENT 112 AN ASSOCIATION OF USER 1 WITH THE ENCRYPTED, HASHED MESSAGE.

320 → IF VALIDATION OF USER KEY 1 IS NEEDED OR DESIRED TO BE REVOKED, VALIDATION OF THE ENCRYPTED, HASHED MSSAGE ASSOCIATED WITH USER 1 CAN BE PREVENTED BY REVOKING ASSOCIATED KEY A ON SERVER SYSTEM 104.

322 → (END)

FIGURE 3

402 → START

403 → COMMUNICATION ESTABLISHED AND MAINTAINED BETWEEN DATA PROCESSING SYSTEM 100 AND RECIPIENT SYSTEM 110.

404 → RECIPIENT SYSTEM 110 RECEIVES FROM CLIENT SYSTEM 102A ENCRYPTED, HASHED MESSAGE, ENCRYPTED USER KEY 1, AND ENCRYPTED ASSOCIATED KEY A TO VALIDATE BY RECIPIENT 112 AN ASSOCIATION OF USER 1 WITH THE ENCRYPTED, HASHED MESSAGE.

408 → RECIPIENT SYSTEM 110 DECRYPTS ENCRYPTED ASSOCIATED KEY A BY ACCESSING AND USING PUECK OF ECK 107.

410 → RECIPIENT SYSTEM 110 DECRYPTS ENCRYPTED USER KEY 1 BY ACCESSING AND USING PUKA OF ASSOCIATED KEY A.

412 → RECIPIENT SYSTEM 110 DECRYPTS THE ENCRYPTED, HASHED MESSAGE BY ACCESSING AND USING PUK1 OF USER KEY 1.

414 → RECIPIENT SYSTEM 110 ACCESSES AND USES SAME CRYPTOGRAPHIC HASH FUNCTION USED BY CLIENT SYSTEM 102A TO HASH THE MESSAGE ATTACHED TO ENCRYPTED, HASHED MESSAGE RECEIVED FROM USER 1.

416 IS HASHED MESSAGE GENERATED BY RECIPIENT SYSTEM 110 SAME AS DECRYPTED HASHED MESSAGE?

418 RECIPIENT SYSTEM 110 NOTIFIES RECIPIENT 112 THAT MESSAGE IS VALID AND VERIFIED AS BEING FROM USER 1.

YES

420 RECIPIENT SYSTEM 110 NOTIFIES RECIPIENT 112 THAT MESSAGE IS NOT VALID AND NOT VERIFIED AS BEING FROM USER 1.

END ←**422**
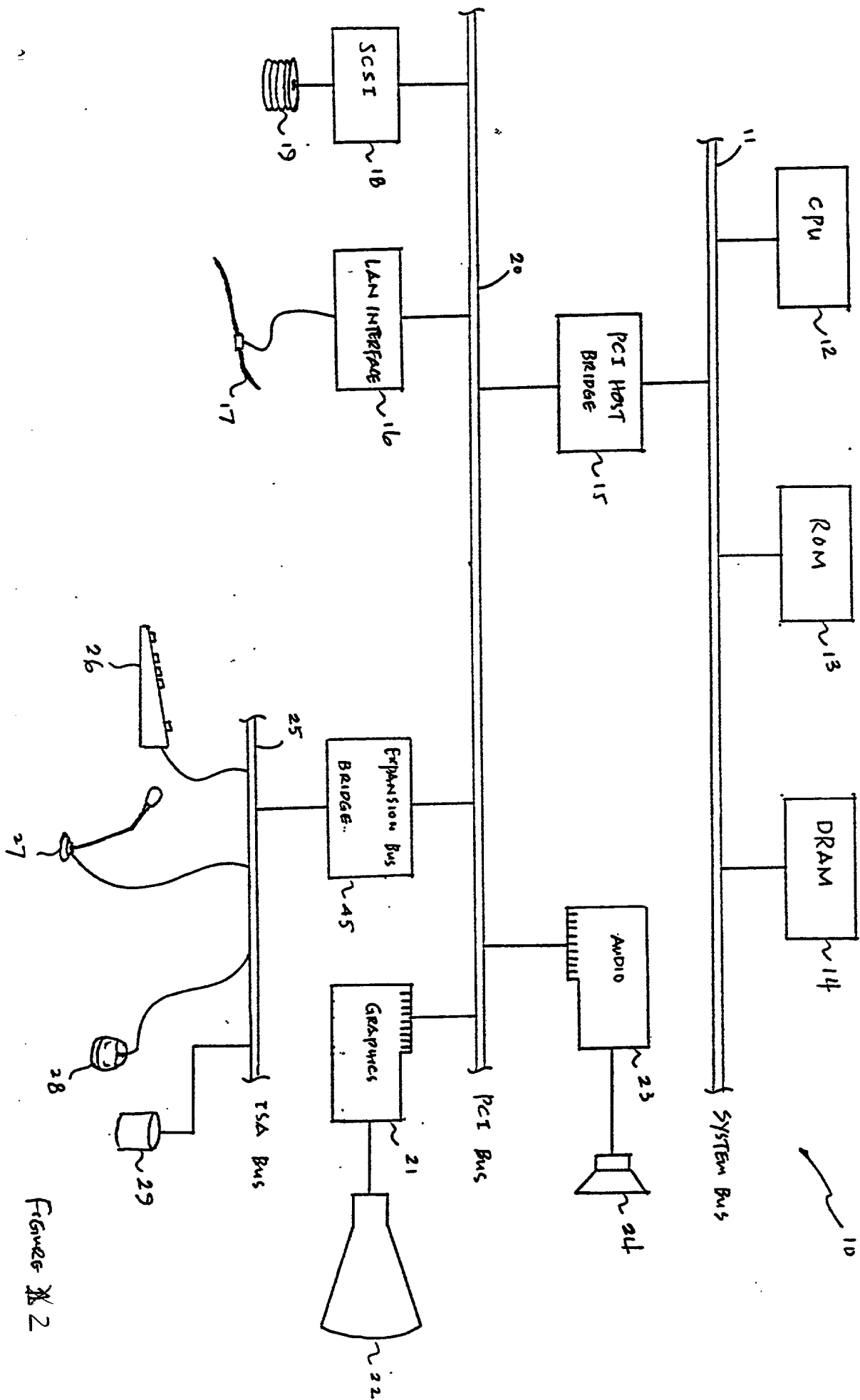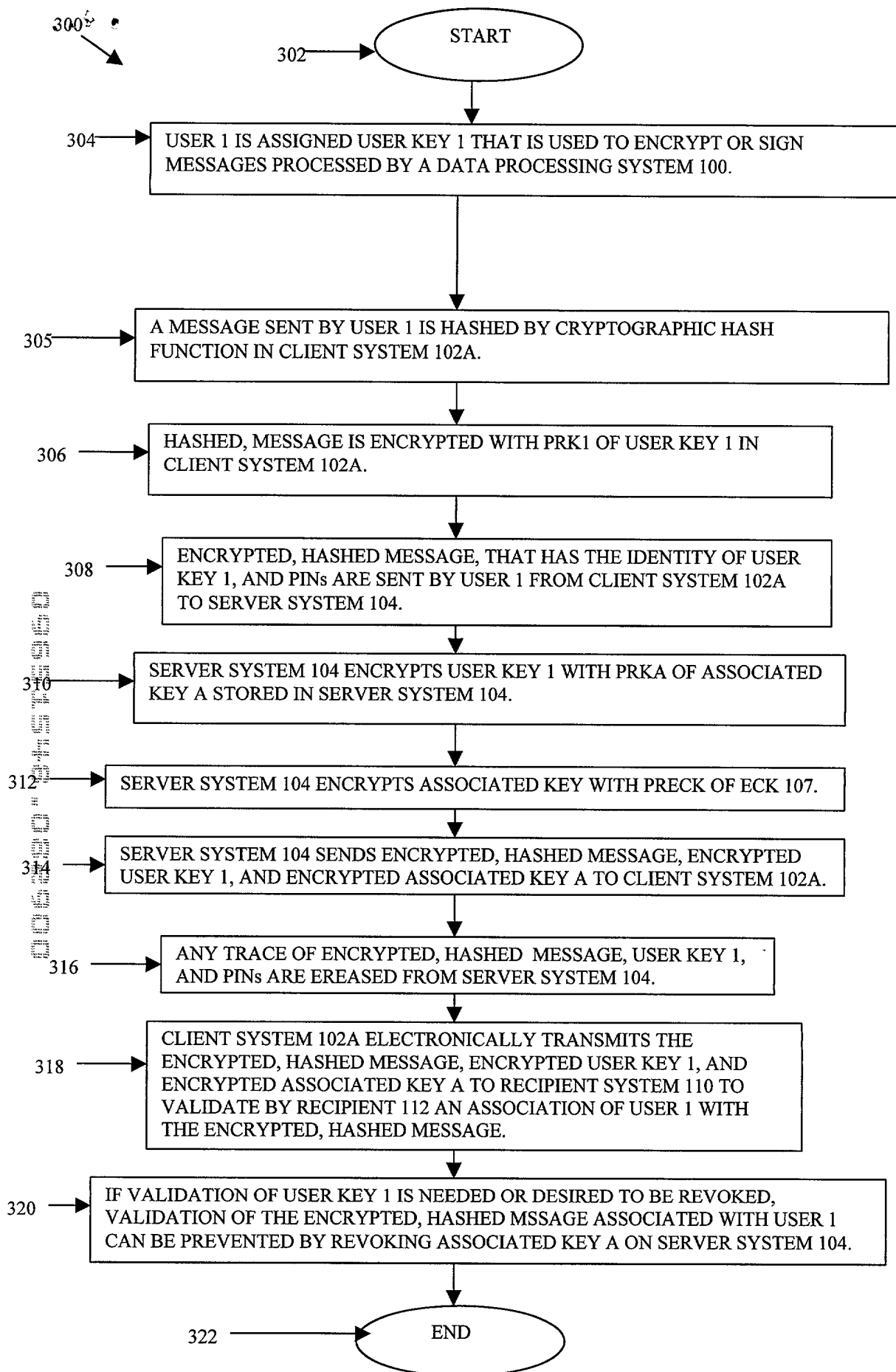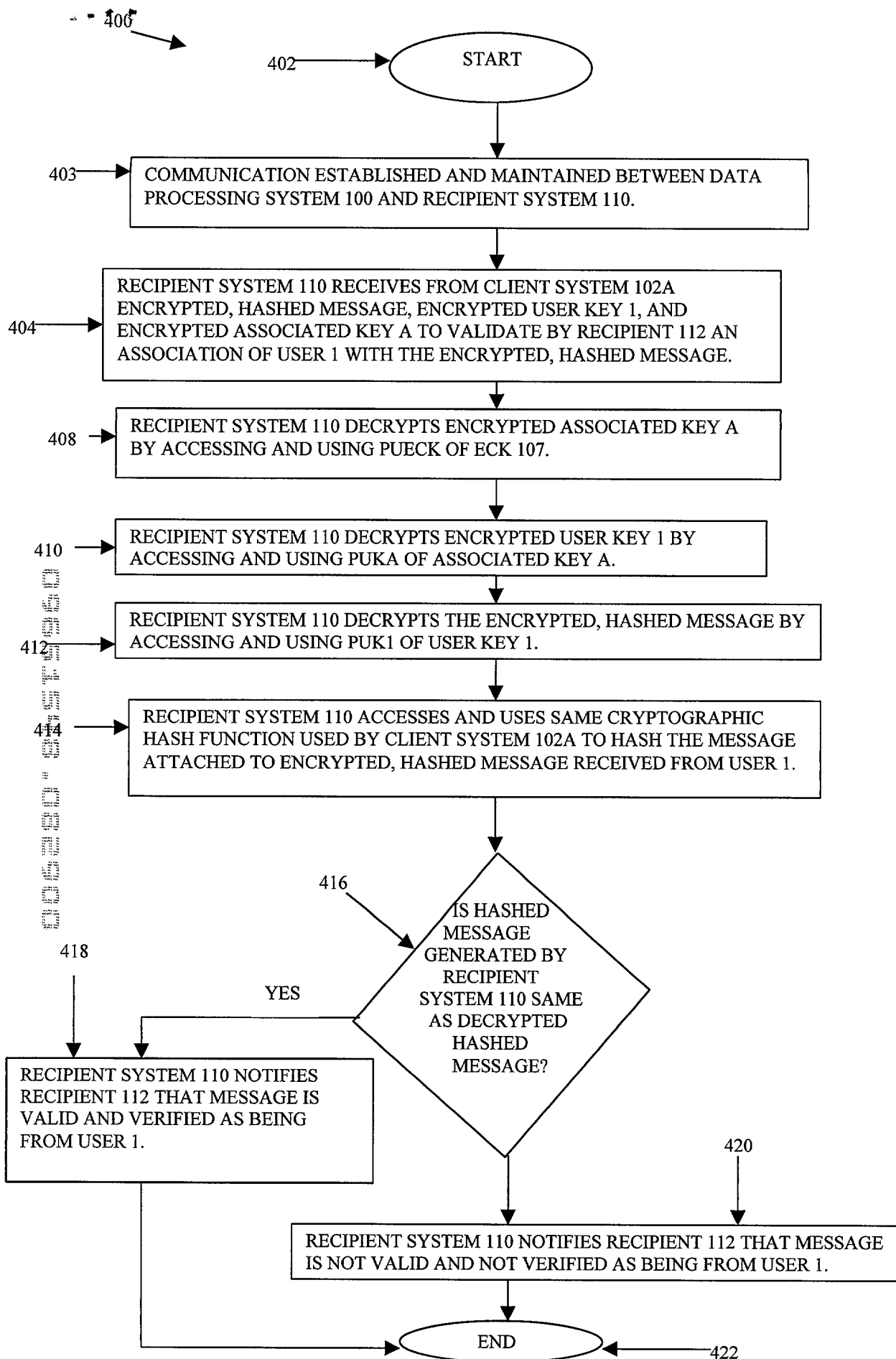
FIGURE 4

DECLARATION AND POWER OF ATTORNEY FOR

PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEM, METHOD, AND PROGRAM FOR MANAGING A USER KEY USED TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM

the specification of which (check one)

X is attached hereto.

__ was filed on _____
   as Application Serial No. _____
   and was amended on _____
                         (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):   Priority Claimed

_____   _____   _____   ___ Yes___ No
   (Number)   (Country)   (Day/Month/Year)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal

statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Horace St. Julian, Reg. No. 30,329; J. Bruce Schelkopf, Reg. No. 43,901; John D. Flynn, Reg. No. 35,137; George E. Grosser, Reg. No. 25,629; Martin J. McKinley, Reg. No. 31,782; Christopher A. Hughes, Reg. No. 26,914; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Andrew J. Dillon, Reg. No. 29,634; Daniel E. Venglarik, Reg. No. 39,409; Jack V. Musgrove, Reg. No. 31,986; Brian F. Russell, Reg. No. 40,796; Matthew W. Baca, Reg. No. 42,277; Antony P. Ng, Reg. No. 43,427; Michael R. Barre, Reg. No. 44,023; Andrew Mitchell Harris, Reg. No. 42,638; Richard McCain, Reg. No. 43,785; and Michael Noe, Jr., Reg. No. 44,975.

Send correspondence to: Andrew J. Dillon ,FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Suite 350 Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon , (512) 343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: <u>Barry Atkins</u>

INVENTORS SIGNATURE:_____ DATE: <u>14 Aug 2000</u>

RESIDENCE: <u>8409 Running Cedar Trail</u>
            <u>Raleigh, North Carolina 27615</u>

CITIZENSHIP: <u>Canadian</u>

POST OFFICE ADDRESS: <u>8409 Running Cedar Trail</u>
                      <u>Raleigh, North Carolina 27615</u>

FULL NAME OF SECOND INVENTOR: David Carroll Challener

INVENTORS SIGNATURE: _____ DATE: 8/17/2000

RESIDENCE: 713 Hunting Ridge Road
Raleigh, North Carolina 27615

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 713 Hunting Ridge Road
Raleigh, North Carolina 27615

FULL NAME OF THIRD INVENTOR: Frank Novak

INVENTORS SIGNATURE: _____ DATE: 21 August 2000

RESIDENCE: 1210-101 New World Circle
Raleigh, North Carolina 27615

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 1210-101 New World Circle
Raleigh, North Carolina 27615

FULL NAME OF FOURTH INVENTOR: Joseph Gary Rusnak

INVENTORS SIGNATURE: _____ DATE: 25 August 2000

RESIDENCE: 4908 Montvale Drive
Durham, North Carolina 27705

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 4908 Montvale Drive
Durham, North Carolina 27705

FULL NAME OF FIFTH INVENTOR: Kenneth D. Timmons

INVENTORS SIGNATURE: _____ DATE: 8/14/2000

RESIDENCE: 11932 Straight-A-Way Lane
Raleigh, North Carolina 27613

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 11932 Straight-A-Way Lane
Raleigh, North Carolina 27613

FULL NAME OF SIXTH INVENTOR: William W. Vetter

INVENTORS SIGNATURE: _____ DATE: _14AUG2000_

RESIDENCE: 7121 Benhart Drive
             Raleigh, North Carolina 27613

CITIZENSHIP: U.S.A._____

POST OFFICE ADDRESS: 7121 Benhart Drive
                       Raleigh, North Carolina 27613